Maryland Wireless Access Policy

Last Updated: 05/17/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is committed to managing the confidentiality, integrity, and availability of information technology assets and information. Implementation of wireless network access offers new challenges in balancing access to information and ensuring security is properly designed and integrated. This policy is based on the NIST standards set forth in the Special Publication series SP800-48R1, SP800-97, and SP800-153, including access controls identified in SP800-53R4.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Appendix C: Wireless Security. This document also supersedes any policy regarding wireless access and security declared prior to the 2017 Cybersecurity Program Policy, such as the DoIT Wireless LAN Security Policy v1.2. This document will be reviewed annually and is subject to revision.

Date	Revision	Policy Updates	Approved By:
01/31/2017	v1.0	Approval of Draft	Maryland CISO
05/17/2017	v1.1	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all agencies supported by, or under the policy authority of, the Maryland Department of Information Technology and using authorized wireless access deployments onsite. The following policy requirements ensure the secure use of wireless technologies while prohibiting unauthorized wireless devices and access points within the network infrastructure.

4.0 Policy

All State of Maryland Executive Branch agencies will ensure all wireless deployments meet the requirements outlined below. To effectively implement a wireless infrastructure, agencies must have a wireless security plan that accounts for the proper deployment of wireless assets as well as for mitigation of the associated risks inherent in these technologies. Agencies directly managed by DoIT with wireless implementations will be monitored through the DoIT Security Operation Center.

Agencies under the policy authority of DoIT, but not under direct management, must independently meet the requirements below and review access and event logs for indications of compromise or improper usage.

Security requirements for mobile devices are outlined in the *Mobile Device Access Policy*.

4.1 Internal Wireless Access

Every agency must have a wireless security plan that establishes mandatory security controls and their implementation requirements before an authorized wireless access point is installed or deployed on its network. The table below identifies the requirements for an agency wireless-access security plan.

	Name	Requirement
A	Wireless Deployment Process	The wireless security plan must have standardized processes and procedures for the consistent configuration, installation, and deployment of authorized, commercial-grade wireless access points.
B	Physical Security	Wireless devices must be installed: ▪ So that unauthorized users are prevented from accessing, tampering with, or damaging the physical devices ▪ Utilizing best practices for optimum signal coverage
C	Perimeter Restriction	Access points must be deployed strategically to minimize or eliminate the signal strength beyond the building perimeter while allowing enough signal overlap so devices within the perimeter can roam available channels. This allows users to move around and maintain a consistent network connection, e.g., moving from cubicle to a meeting room.
D	Authorization Requirements	For internal Local Area Network (LAN) deployments (accessing confidential, internal resources): ▪ Wireless access points will be designed to require both device verification and user authentication ▪ Wireless networks will be segmented to prevent unauthorized connections from scanning or accessing other internal segments, i.e., preclude lateral movement across wireless segments
E	Trust Level Separation	Deployment of wireless access points must account for and restrict access based on established trust levels, e.g., guest wireless service cannot access internal resources or data.
F	Segmentation	Any guest wireless access point must be *completely segmented from the internal LAN* and all connection attempts, direct or lateral, from the guest segment to the LAN must be prevented. No cross connection or bridge will be permitted.
G	Security Requirements	All access points must: ▪ Utilize the latest security and encryption features, including passwords with strong **entropy** ▪ Change default administrator credentials ▪ Change default **SSID** ▪ Disable **SNMP** (or change the default string if utilized and require the latest encrypted version) ▪ Use an authentication protocol like variants of Extensible Authentication Protocol (EAP) or use a RADIUS server ▪ Incorporate event-logging and log-forwarding to the DoIT Security Operations Center (for Enterprise onboarded agencies) ▪ Require mobile device security verification, e.g., ensure endpoint security is enabled and up to date and device is scanned before allowing access to internal resources (e.g., Network Access Control or Mobile Device Management implementation)

	Name	Requirement
H	Bandwidth Saturation	Any internal LAN connections that require heavy and consistent data transfers shall be prohibited from using the wireless LAN and instead shall be connected via Ethernet cable to the network.

4.2 Guest Wireless Access

Agencies might require guest wireless services for visitors or as a courtesy to the public. This constitutes an untrusted connection and must be explicitly placed in the DMZ — with no access to any internal network resource. The wireless security plan must ensure network separation for guest Internet-access deployments.

The guest acceptable use and disclaimer notice is provided in Appendix A of this policy and should be posted conspicuously in areas where guest wireless may be available.

All State employees, agency supporting contractors and vendors, and other individuals and entities with authorized agency credentials who connect to a guest wireless access point (e.g., utilizing personal devices) will be bound by the requirements set forth in the acceptable use form (see *Acceptable Use Policy*).

4.3 Wireless Security Threats

The following table identifies common threats against wireless access points and devices. The wireless security plan will use defense-in-depth strategies to mitigate or eliminate these threats before deploying wireless, internal LAN access points or devices to an agency.

	Name	Requirement
A	Eavesdropping	An adversary may attempt to capture wireless packets from the air, such as using a receiver while sitting in a parking lot nearby. Defense strategy: Using the latest encryption and network authentication methods helps prevent these kinds of attacks.
B	Tampering	An attacker may attempt to capture or modify information while in transit. Defense strategy: While more difficult to detect from an insider threat, implementing encryption will prevent outside sources from tampering with the integrity of the data.
C	Unauthorized Access	Adversaries may use the wireless access point to gain entry to the internal network. Defense strategy: Proper network segmentation and strict separation of guest networks from internal LAN resources will diminish resources available to an adversary.
D	Spoofing	An attacker may reconfigure hardware and software settings to mimic an authorized device to gain access to the internal network. Defense strategy: Using multiple security measures will help prevent an unauthorized client from authenticating to the network.
E	Denial of Service	An adversary may flood the access point with traffic, causing the access point to reset and prohibit authorized clients from connecting.

	Name	Requirement
F	Rogue Access Points	An adversary or even an unintentional user may connect an unauthorized access point to the network, e.g., using a device like a USB wireless access point on an authorized client. Defense strategy: Restricting USB access only to users with job duties requiring it can help mitigate this threat.
G	Evil Twin	Setting up another wireless station with the same SSID broadcasting with a stronger signal can cause authorized clients to "de-auth", or disconnect from the existing network, and attempt to reconnect to the "evil twin", thereby providing credential information or the ability to funnel the client traffic through the adversary's device for capture. Defense strategy: Requiring both client and network authentication, such as EAP, will help prevent clients from connecting to an evil twin.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy, then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The *Cybersecurity Program Policy* mandates this policy. Other related policies include:

- Acceptable Use Policy
- Boundary Protection and Internet Access Policy
- Mobile Device Access Policy

7.0 Definitions

Term	Definition
Entropy	A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret.
Simple Network Management Protocol (SNMP)	Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
Service Set Identifier (SSID)	A sequence of characters that uniquely names a wireless local area network (WLAN).

8.0 Enforcement

The Maryland Department of Information Technology is responsible for managing access to information technology assets of Enterprise onboarded agencies. Agencies under the policy

authority but not directly managed by DoIT will comply with the requirements outlined in section 4.0 of this policy unless an agency has completed a Policy Exemption Request Form and received approval from DoIT.

If DoIT determines that an agency is not compliant with the *Wireless Access Policy*, the agency will be given sixty (60) days to become compliant per the requirements in this policy. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated.

Any attempt to circumvent this policy, e.g., installing a rogue access point or tethering a Maryland State asset to an unauthorized connection, will be considered a security violation and may be subject to disciplinary action to include written notice, suspension, termination, and possible criminal and/or civil penalties.

Appendix A: Acceptable Use for Wireless Guests — Public Notice

General Usage Wireless Access Policy

This agency of the State of Maryland may provide free Internet access for guests using mobile WiFi-enabled devices such as cell phones and laptops. This notice is posted as an acceptable use policy; signing in to the provided wireless access point implies the user's agreement to acceptable use behavior and consent to monitoring by access-point owners.

- Access is not guaranteed and use of the wireless access is provided as a courtesy by this agency. The agency reserves the right to deny or terminate access at any time.
- This agency provides guest access as-is and *will provide no technical assistance for guests*.
- Guest Internet access is *untrusted*, and users are warned to use due care while using guest Internet access, e.g., avoid submitting credit card or user ID and password information over the connection.
- The State is not responsible for protecting the privacy of guest users on this wireless Internet connection, and the users assume all risks and responsibility for protecting their personal information.

Acceptable Use

The State has a management responsibility to enforce appropriate use of guest access provided by this agency. All users are expected to use the wireless access in a legal and responsible manner and avoid violating Federal, State of Maryland, or local laws, including those relating to:

- The transmission or receipt of any pornography or similarly harmful material — Accessing, using, or displaying obscene language or sexually explicit graphics or materials is prohibited.
- Fraud — Users are prohibited from misrepresenting themselves as another user; attempting to modify or gain access to files, passwords, or data belonging to others; seeking unauthorized access to any computer system; or damaging or altering software components of any network or database.
- Downloading copyrighted material — U.S. Copyright law prohibits the unauthorized reproduction or distribution of copyrighted materials, except as permitted by the principles of "fair use." No user may copy or distribute electronic materials without the explicit permission of the copyright holder.

By connecting to this wireless access network the user agrees to abide by all laws and all rules and regulations of the State of Maryland and the Federal Government applicable to Internet use.

Disclaimer

This agency provides guest-wireless connectivity as a courtesy and offers no guarantees or representations that use of this wireless connection is in anyway secure, or that privacy can be protected when using this wireless connection. Use of this wireless connection is entirely at the risk of the user, and the State is not responsible for the loss of any information that may arise from the use of this wireless connection; nor is the State responsible for any loss, injury, or damage resulting from the use of this wireless connection.